CLAIMS

1. A method comprising:

receiving an encrypted data packet through a wireless communication channel;

decrypting the encrypted data packet to produce a decrypted data packet at a security sub-network layer;

at a network layer, calculating a payload checksum based on a payload of the decrypted data packet; and

comparing a received network layer header checksum within a network layer header of the decrypted data packet to the payload checksum to determine an integrity of the payload.

2. A method in accordance with claim 1, further comprising:

determining the payload is not valid if the payload checksum does not equal the received network layer header checksum.

3. A method in accordance with claim 1, further comprising:

receiving the encrypted data packet at a data link layer, the data link layer providing communications through the wireless communication channel; and

transferring the encrypted data packet to the sub-network security layer.

4. A method in accordance with claim 3, further comprising:

resetting the data link layer if the payload checksum does not equal the received network layer header checksum.

5. A method in accordance with claim 1, further comprising:

prior to receiving the encrypted data packet, calculating a transmitter payload checksum based on the payload at the network layer;

comparing the transmitter payload checksum to the network layer header checksum at the network layer;

forming the encrypted data packet using the payload and the network layer header checksum; and

transmitting the encrypted data packet through the wireless channel at the data link layer.

6. A method in accordance with claim 5, wherein the forming comprises:

encrypting the payload and the network layer header checksum.

7. A method for key stream out-of-synchronization detection comprising:

encrypting data in accordance with a network layer checksum to produce encrypted payload data having an embedded checksum;

receiving the encrypted payload data at a receiver; and

comparing the encrypted payload data to the network layer checksum to detect the key stream out-of-synchronization.

8. A method in accordance with claim 7, wherein the encrypting comprises:

encrypting, at a sub-network security layer, a data packet comprising the network layer checksum and a payload data to form the encrypted payload data.

9. A method in accordance with claim 8, further comprising:

transmitting the encrypted payload data through a wireless channel at a data link layer.

10. A method in accordance with claim 7, wherein the comparing comprises:

decrypting, using a key stream, the encrypted payload data to produce decrypted payload data and a received checksum,

calculating a calculated checksum based on the decrypted payload data; and

detecting, at the network layer, the key stream loss of synchronization if the calculated checksum is not equal to the received checksum.

11. A receiver comprising:

a decryption engine adapted to decrypt, at a security sub-network layer, an encrypted data packet received through a wireless communication channel to produce a decrypted data packet ;

a checksum generator configured to calculate, at a network layer, a payload checksum based on a payload of the decrypted data packet; and

a checksum validation engine configured to compare a received network layer header checksum within a network layer header of the decrypted data packet to the payload checksum to determine an integrity of the payload.

12. A receiver in accordance with claim 11, the checksum validation engine further configured to determine the payload is not valid if the network layer header checksum does not equal the received network layer header checksum.

13. A receiver in accordance with claim 11, wherein the decryption engine is further configured to receive the encrypted data packet at a data link layer, the data link layer providing communications through the wireless communication channel to transfer the encrypted data packet to the sub-network security layer.

14. A receiver in accordance with claim 13, the checksum validation engine further configured to reset the data link layer if the payload checksum does not equal the received network layer header checksum.

15. A communication system comprising:

a transmitter checksum generator configured to calculate a transmitter payload checksum based on a payload at a network layer; and

a transmitter checksum validation engine configured to compare the

transmitter payload checksum to a transmitter network layer checksum at the network layer.

16. A system in accordance with claim 15 further comprising:

a transmitter encryption engine configured to encrypt the payload at the transmitter network layer checksum to form the encrypted data packet;

17. A system in accordance with claim 16 further comprising:

a transmitter configured to transmit the encrypted data packet through the wireless channel at the a data link layer.

18. A system for key stream out-of-synchronization detection comprising:

an encryption engine configured to encrypt payload data in accordance with a network layer checksum to produce encrypted payload data having an embedded checksum;

a transmitter configured to transmit the encrypted payload data through a wireless channel to a decryption engine; and

a decryption engine configured to decrypt the encrypted payload data and a checksum validation engine configured to compare the encrypted payload data to the network layer checksum to detect the key stream out-of-synchronization.

19. A system in accordance with claim 18, wherein the encryption engine is further configured to encrypt, at a sub-network security layer, a data packet comprising the network layer checksum and a payload data to form the encrypted payload data.

20. A system in accordance with claim 19, the transmitter further configured to transmit the encrypted payload data through a wireless channel at a data link layer.

21. A system in accordance with claim 20, wherein the checksum validation engine comprises:

a decryption engine configured to decrypt, using a key stream, the encrypted payload data to produce decrypted payload data and a received checksum; and

a checksum generator configured to calculate a calculated checksum based on the decrypted payload data; the checksum validation engine configured to detect, at the network layer, the key stream loss of synchronization if the calculated checksum is not equal to the received checksum.

22. An apparatus comprising:

a checksum generator configured to calculate a transmitter payload checksum based on a payload at a network layer;

a checksum validation engine configured to compare the transmitter payload checksum to the transmitter network layer check sum at the network layer;

an encryption engine configured to encrypt the payload at the transmitter network layer checksum to form the encrypted data packet; and

a transmitter adapted to transmit the encrypted data packet to a receiver.

23. An apparatus in accordance with claim 22, wherein the transmitter is further adapted to transmit the encrypted data packet through a wireless communication channel.

24. A method of determining the integrity of a payload of a decrypted data packet, the method comprising:

at a network layer, calculating a payload checksum based on the payload; and

comparing a received network layer header checksum within a network layer header of the decrypted data packet to the payload checksum.

25. A method in accordance with claim 24 further comprising:

receiving the encrypted data packet through a wireless communication channel.

26. A method in accordance with claim 25 further comprising:

decrypting the encrypted data packet to produce a decrypted data packet at a security sub-network layer.

27. A receiver having a decryption engine, the receiver comprising:

a checksum generator configured to calculate, at a network layer, a payload checksum based on a payload of a decrypted data packet; and

a checksum validation engine configured to compare a received network layer header checksum within a network layer header of the decrypted data packet to the payload checksum to determine an integrity of the payload.

28. A receiver in accordance with claim 27, further comprising:

a decryption engine adapted to decrypt, at a security sub-network layer,

a encrypted data packet received through a wireless communication channel to produce the decrypted data packet.